Claims:

1. (Previously Presented) An article of manufacture including a sequence of instructions stored on a computer-readable media which when executed by a computer network node cause the network node to perform the acts of:

analyzing computer data transmissions with the instructions to determine type, destination, and origin of data contained in the computer data transmissions in order to classify the data according to one or more categories;

modifying an alert variable based on the computer data transmissions originating from one or more suspect computer nodes comprising workstations;

triggering a first response when said alert variable reaches a first predetermined threshold level; and

triggering a second response when said alert variable reaches a second predetermined threshold level.

2. (Original) The article of manufacture as claimed in claim 1 further including the step of triggering additional responses when said alert variable reaches one or more additional threshold levels.

3. (Previously Presented) The article of manufacture as claimed in claim 1 wherein one of said triggered responses includes a passive scan of one or more of said suspect computer nodes.

4. (Previously Presented) The article of manufacture as claimed in claim 3 wherein said passive scan includes the step of recording the computer data transmissions in a log file.

5. (Previously Presented) The article of manufacture as claimed in claim 1 wherein one of said triggered responses includes an active scan of one or more of said suspect computer nodes.

6. (Previously Presented) The article of manufacture as claimed in claim 5 wherein said active scan includes the step of retrieving information about one or more of said suspect computer nodes including the network address of said suspect computer nodes.

7. (Previously Presented) The article of manufacture as claimed in claim 5 wherein said active scan includes the step of determining the network route taken by data originating from one or more of said suspect computer nodes.

8. (Previously Presented) The article of manufacture as claimed in claim 1 wherein one of said triggered responses includes said computer network node requiring increased authentication from any other computer node before providing access to its resources.

9. (Original) The article of manufacture as claimed in claim 8 wherein said increased authentication includes the step of forcing two or more logins before providing access to its resources.

10. (Previously Presented) The article of manufacture as claimed in claim 1 wherein one of said triggered responses includes the step of blocking incoming computer data transmissions.

11. (Previously Presented) The article of manufacture as claimed in claim 1 wherein said alert variable responds differently over time to particular types of computer data transmissions.

12. (Previously Presented) The article of manufacture as claimed in claim 11 wherein said alert variable continuously increases in response to the continuous receipt of a particular type of computer data transmission until the alert variable reaches a predetermined value.

13. (Previously Presented) The article of manufacture as claimed in claim 12 wherein said particular type of computer data transmission originating from said suspect computer node is an invalid login attempt.

14. (Previously Presented) The article of manufacture as claimed in claim 11 wherein said alert variable initially increases in response to the continuous receipt of a particular type of computer data transmission and subsequently decreases in response to the continued receipt of said particular type of computer data transmission.

15. (Previously Presented) The article of manufacture as claimed in claim 14 wherein said particular type of computer data transmission originating from said suspect computer node is a computer data transmission which retrieves information about said computer network node.

16. (Previously Presented) The article of manufacture as claimed in claim 1 wherein said computer data transmissions are analyzed by said computer network node on a network packet level.

17. (Previously Presented) The article of manufacture as claimed in claim 16 wherein said computer data transmissions are filtered by said computer network node on a network packet level.

[The remainder of this page has been intentionally left blank.]

18. (Previously Presented) An article of manufacture including a sequence of instructions stored on a computer-readable media which when executed by a computer network node cause the computer network node to perform the acts of:

with the sequence of instructions, analyzing computer data transmissions comprising non-voice based data to determine type and origin of data contained in the computer data transmissions in order to classify the data according to one or more categories;

modifying a first suspect-specific alert variable based on the computer data transmissions originating from a first suspect computer node comprising a workstation;

modifying a second suspect-specific alert variable based on the computer data transmissions originating from a second suspect computer node comprising a workstation; and

triggering a suspect-specific response when either of said suspect-specific alert variables reach a predetermined threshold level.

19. (Original) The article of manufacture as claimed in Claim 18 including the act of triggering additional suspect-specific responses when either of said suspect-specific alert variables reaches additional predetermined threshold values.

20. (Previously Presented) The article of manufacture as claimed in claim 18 including the act of modifying an overall alert variable based on said computer data transmissions originating from each of said suspect computer nodes.

21. (Previously Presented) The article of manufacture as claimed in claim 20 including the act of triggering a response towards each one of said plurality of suspect computer nodes when said overall alert variable reaches a predetermined threshold value.

22. (Previously Presented) The article of manufacture as claimed in claim 20 wherein said overall alert variable is more responsive to new types of computer data transmissions than to computer data transmissions previously received at said computer network node.

23. (Previously Presented) The article of manufacture as claimed in claim 22 including the act of initially increasing said overall alert variable in response to the computer data transmissions originating from a particular suspect computer node and subsequently decreasing said overall alert variable upon continued receipt of said computer data transmissions from said particular suspect computer node.

24. (Previously Presented) The article of manufacture as claimed in claim 18 including the act of communicating each of said suspect-specific alert variables to a network database residing on a computer server node.

25. (Previously Presented) The article of manufacture as claimed in claim 20 including the act of communicating said overall alert variable to a network database residing on a computer server node.

[The remainder of this page has been intentionally left blank.]

26. (Currently Amended) An article of manufacture including a sequence of instructions stored on a computer-readable media which when executed by a computer network server node cause the computer network server node to perform the acts of:

storing a plurality of suspect-specific alert variables for a plurality of computer network nodes comprising workstations;

modifying a network alert variable based on the value of each of said plurality of suspect-specific alert variables; and

triggering a network response when said network alert variable reaches a predetermined threshold level, wherein the network response comprises notifying each of the plurality of computer network nodes that they should each increase their suspect-specific alert variable towards a particular suspect computer node and initiating an active scan of the particular suspect computer node.

27. (Cancelled).

28. (Currently Amended) The article of manufacture as claimed in claim [[27]]26, wherein said network response includes the act of said computer network server node initiating a passive scan of [[a]] the particular suspect computer node.

29. (Cancelled).

30. (Currently Amended) The article of manufacture as claimed in claim [[29]]26, wherein said network response includes the act of blocking all communication between said suspect computer node and said plurality of computer network nodes.

[The remainder of this page has been intentionally left blank.]

31. (Cancelled).

32. (Previously Presented) A method comprising:

with a sequence of instructions in software, analyzing a first event from a suspect computer node comprising a workstation to determine type, destination, and origin of data contained in the event without using pattern alarms;

recording said first event in a first data structure having an event count value;

with the sequence of instructions in software, analyzing a second event from said computer suspect node to determine type, destination, and origin of data contained in the event without using pattern alarms, said second event being of a same type as said first event; and

recording said second event in said first data structure and incrementing said count value if said second event occurs within a predetermined window of time after said first event.

33. (Original) The method as claimed in claim 32 further comprising recording said second event in a second data structure having a count value if said second event occurs outside of said predetermined window of time after said first event.

34. (Original) The method as claimed in claim 33 wherein said predetermined window of time is increased responsive to said second event occurring outside of said predetermined window of time.

35. (Original) The method as claimed in claim 32 wherein said predetermined window of time is modified based on said first or second event type.

36. (Original) The method as claimed in claim 35 wherein said window of time is increased for more serious event types and decreased for less serious event types

37. (Original) The method as claimed in claim 36 wherein said event type is an invalid login.

38. (Original) The method as claimed in claim 36 wherein said event type is a ping.

39. (Original) The method as claimed in claim 32 further comprising generating a report of all new events which occur over a predetermined time period.

40. (Previously Presented) The method as claimed in claim 39 wherein an event is identified as a new event by:

determining whether said event is included in a single data structure with one or more pervious events received in a time period preceding said predetermined time period;

searching all data structures generated during said time period preceding said predetermined time period if said event is not included in said single data structure with one or more previous events; and

including said event in said report if said event is not identified in any data structures generated during said time period preceding said predetermined time period.

[The remainder of this page has been intentionally left blank.]